

TUGAS JARINGAN KOMPUTER

Analisis Paket Data dengan Menggunakan Wireshark dan Command Prompt



Nama : Endi Kumara

NIM : 09011281520098

Kelas : SK5 C

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

I. Pengertian Wireshark

Wireshark merupakan salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya termasuk protokol didalamnya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data atau informasi yang berseliweran dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya. Wireshark dipakai oleh network administrator untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan yang terlihat dan semua jenis informasi ini dapat dengan mudah dianalisa yaitu dengan memakai sniffing , dengan sniffing diperoleh informasi penting seperti password email account lain. Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan.

II. Pengertian Command Prompt (CMD)

CMD (Command Prompt) adalah sebuah perintah dos yang terdapat pada Windows yang bisa memudahkan pengguna dalam menjelajahi windows secara online maupun offline.

III. Tabel IP Source dan IP Destinatiion

- www.kompas.com

TABEL (www.kompas.com)		
Source		
IP Source	IP Destination	
192.168.1.101	202.146.4.100	[TCP Keep-Alive] 49957 → 80 [ACK] Seq=383 Ack=21679 Win=64860 Len=1
192.168.1.101	202.146.4.100	49957 → 80 [ACK] Seq=384 Ack=12741 Win=64860 Len=0
192.168.1.101	202.146.4.100	[TCP Dup ACK 1369#1] 49957 → 80 [ACK] Seq=384 Ack=1 Win=64240 Len=0 SLE=1381 SRE=2761
192.168.1.101	202.146.4.100	49957 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.1.101	202.146.4.100	49957 → 80 [ACK] Seq=384 Ack=2761 Win=64860 Len=0
Destination		
IP Source	IP Destination	
202.146.4.100	192.168.1.101	[TCP Keep-Alive ACK] 80 → 49957 [ACK] Seq=21679 Ack=384 Win=4523 Len=0
202.146.4.100	192.168.1.101	80 → 49957 [ACK] Seq=12741 Ack=384 Win=4523 Len=1380
202.146.4.100	192.168.1.101	[TCP Out-Of-Order] 80 → 49957 [ACK] Seq=1 Ack=384 Win=4523 Len=1380
202.146.4.100	192.168.1.101	80 → 49957 [ACK] Seq=1 Ack=384 Win=4523 Len=0
202.146.4.100	192.168.1.101	80 → 49957 [PSH, ACK] Seq=2761 Ack=384 Win=4523 Len=320

- www.lk21.net

A	B	C	E
TABEL (lk21.net)			
Source			
IP Source	IP Destination		
192.168.1.101	104.31.72.126	52307 → 80 [ACK] Seq=504 Ack=8365 Win=66816 Len=0 SLE=13941 SRE=15335	
192.168.1.101	104.31.72.127	52307 → 80 [ACK] Seq=504 Ack=9759 Win=66816 Len=0 SLE=11153 SRE=12547 SLE=13941 SRE=15335	
192.168.1.101	104.31.72.128	52307 → 80 [ACK] Seq=504 Ack=12547 Win=66816 Len=0 SLE=13941 SRE=15335	
192.168.1.101	104.31.72.129	52307 → 80 [ACK] Seq=504 Ack=15335 Win=66816 Len=0	
192.168.1.101	104.31.72.130	[TCP Dup ACK 733#1] 52307 → 80 [ACK] Seq=504 Ack=15335 Win=66816 Len=0 SLE=16729 SRE=18123	
Destination			
IP Source	IP Destination		
104.31.72.126	192.168.1.101	[TCP Retransmission] 80 → 52307 [ACK] Seq=11153 Ack=504 Win=30720 Len=1394	
104.31.72.127	192.168.1.101	[TCP Retransmission] 80 → 52307 [ACK] Seq=9759 Ack=504 Win=30720 Len=1394	
104.31.72.128	192.168.1.101	[TCP Retransmission] 80 → 52307 [ACK] Seq=12547 Ack=504 Win=30720 Len=1394	
104.31.72.129	192.168.1.101	[TCP Previous segment not captured] 80 → 52307 [ACK] Seq=16729 Ack=504 Win=30720 Len=1394	
104.31.72.130	192.168.1.101	80 → 52307 [ACK] Seq=18123 Ack=504 Win=30720 Len=1394	

IV. Analisis Wireshark dan Command Prompt

- ❖ www.kompas.com

The image shows two windows side-by-side. The top window is Wireshark, displaying a list of network packets. The bottom window is a Windows Command Prompt showing the output of the 'netstat -a' command, listing active connections.

No.	Time	Source	Destination	Protocol	Length	Info
4052	92.455872	74.125.130.84	192.168.1.101	TCP	66	[TCP Keep-Alive ACK] 443 → 52008 [ACK] Seq=5176 Ack=1176 Win=50432 Len=0 SLE=1175 SRE=1176
4053	92.577805	192.168.1.101	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1c>
4054	93.328234	192.168.1.101	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1c>
4055	93.487510	192.168.1.101	74.125.130.84	TCP	55	[TCP Keep-Alive] 52011 → 443 [ACK] Seq=654 Ack=4268 Win=65536 Len=1
4056	93.566012	74.125.130.84	192.168.1.101	TCP	66	[TCP Keep-Alive ACK] 443 → 52011 [ACK] Seq=4268 Ack=655 Win=45056 Len=0 SLE=654 SRE=655
4057	93.862591	Shenzhen_28:a4:5a	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.1
4058	93.972935	192.168.1.101	54.231.120.227	TCP	55	[TCP Keep-Alive] 52063 → 443 [ACK] Seq=0 Ack=9 Win=66816 Len=1
4059	94.277370	54.231.120.227	192.168.1.101	TCP	54	[TCP Keep-Alive ACK] 443 → 52063 [ACK] Seq=9 Ack=1 Win=14848 Len=0
4060	94.386413	Shenzhen_28:a4:5a	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.1
4061	95.144558	192.168.1.101	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1c>
4062	95.436575	192.168.1.101	172.217.27.36	TCP	55	[TCP Keep-Alive] 52016 → 443 [ACK] Seq=649 Ack=4228 Win=65792 Len=1
4063	95.618384	172.217.27.36	192.168.1.101	TCP	66	[TCP Keep-Alive ACK] 443 → 52016 [ACK] Seq=4228 Ack=650 Win=47104 Len=0 SLE=649 SRE=650
4064	95.808320	Shenzhen_28:a4:5a	Broadcast	ARP	42	Who has 192.168.1.102? Tell 192.168.1.1
4065	95.894145	192.168.1.101	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1c>
4066	96.645076	192.168.1.101	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1c>


```

> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
> Ethernet II, Src: Azurewaw_c9:8e:cf (74:c6:3b:c9:8e:cf), Dst: Shenzhen_28:a4:5a (fc:dd:55:28:a4:5a)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 49376 (49376), Dst Port: 53 (53)

0000  fc dd 55 28 a4 5a 74 c6 3b c9 8e cf 00 00 45 00  ..U(.Zt. j....E.
0010  00 40 2b a4 00 00 00 11 8b 52 c0 a8 01 65 c0 a8  .@#. .... .R...e.
0020  01 01 c0 e0 00 35 00 2c 06 d3 de f3 01 00 00 01  ....5j. ....
0030  00 00 00 00 00 04 61 75 74 68 09 67 72 61 6d  ....a.uth.gram
0040  6d 61 72 6c 79 83 63 6f 6d 00 00 01 00 01  ....marly.co m.....

```



```

C:\WINDOWS\system32>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135              ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:445              ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:1688             ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:49664            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:49665            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:49666            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:49667            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:49668            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    0.0.0.0:49670            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    127.0.0.1:9990            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    127.0.0.1:49071          ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    192.168.1.101:139        ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    192.168.1.101:40735     ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP    192.168.1.101:49684     hk2sch130020761:https ESTABLISHED
TCP    192.168.1.101:49800     111.221.77.142:40027 ESTABLISHED
TCP    192.168.1.101:49802     91.190.218.55:12350 ESTABLISHED
TCP    192.168.1.101:49957     202.146.4.100:http TIME_WAIT
TCP    192.168.1.101:49964     sin1i03-in-f42:https TIME_WAIT
TCP    192.168.1.101:49972     104.20.52.12:https TIME_WAIT
TCP    192.168.1.101:50003     202.61.113.151:http TIME_WAIT
TCP    192.168.1.101:50015     202.61.113.71:http TIME_WAIT
TCP    192.168.1.101:50021     sb-in-f132:https TIME_WAIT
TCP    192.168.1.101:50039     202.61.113.71:http TIME_WAIT
TCP    192.168.1.101:50055     sa-in-f94:https ESTABLISHED
TCP    192.168.1.101:50066     sc-in-f108:5228 ESTABLISHED
TCP    192.168.1.101:50067     sc-in-f94:https ESTABLISHED
TCP    192.168.1.101:50068     sc-in-f95:https ESTABLISHED
TCP    192.168.1.101:50069     sp-in-f95:https ESTABLISHED
TCP    192.168.1.101:50070     sa-in-f130:https ESTABLISHED
TCP    192.168.1.101:50072     sb-in-f91:https ESTABLISHED
TCP    192.168.1.101:50074     ec2-54-85-142-199:https TIME_WAIT
TCP    192.168.1.101:50077     ec2-52-206-2-232:https LAST_ACK
TCP    192.168.1.101:50078     ec2-52-206-2-232:https TIME_WAIT
TCP    192.168.1.101:50112     sa-in-f103:https ESTABLISHED
TCP    192.168.1.101:50114     sc-in-f101:https ESTABLISHED
TCP    192.168.1.101:50115     ec2-52-206-2-232:https ESTABLISHED
TCP    192.168.1.101:50117     sc-in-f94:https ESTABLISHED
TCP    192.168.1.101:50121     202.146.4.100:http TIME_WAIT
TCP    192.168.1.101:50122     server-54-230-156-101:http TIME_WAIT

```

Analisis: setelah melihat data dari wireshark dan command prompt terlihat pada wireshark lebih detail dalam memberikan info paket data yg berupa ip source, ip destination, protocol, length, info, time, dan nomor. Sedangkan pada CMD hanya berupa protocol, ip source, address, dan state. Dengan menggunakan wireshark kita bisa mengetahui info yang terdapat di dalam paket data tersebut.

Wireshark interface showing network traffic capture. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 9959) is highlighted in green. The packet list shows a sequence of TCP segments from 192.168.1.101 to 192.168.1.101. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields. The packet bytes pane shows the raw hex and ASCII data.

```

Administrator: Command Prompt
C:\WINDOWS\system32>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP 0.0.0.0:135              ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:445              ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:1688            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:2869            ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:49664           ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:49665           ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:49666           ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:49667           ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:49668           ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 0.0.0.0:49679           ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 127.0.0.1:1688          ASUS-A456UR-IS-VGA-WIN10:52345 ESTABLISHED
TCP 127.0.0.1:19990         ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 127.0.0.1:10400         ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 127.0.0.1:10401         ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 127.0.0.1:10402         ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 127.0.0.1:10402         ASUS-A456UR-IS-VGA-WIN10:52354 ESTABLISHED
TCP 127.0.0.1:49671         ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 127.0.0.1:50509         ASUS-A456UR-IS-VGA-WIN10:50510 ESTABLISHED
TCP 127.0.0.1:50510         ASUS-A456UR-IS-VGA-WIN10:50509 ESTABLISHED
TCP 127.0.0.1:50512         ASUS-A456UR-IS-VGA-WIN10:50513 ESTABLISHED
TCP 127.0.0.1:50513         ASUS-A456UR-IS-VGA-WIN10:50512 ESTABLISHED
TCP 127.0.0.1:52300         ASUS-A456UR-IS-VGA-WIN10:10402 TIME_WAIT
TCP 127.0.0.1:52341         ASUS-A456UR-IS-VGA-WIN10:10402 TIME_WAIT
TCP 127.0.0.1:52345         ASUS-A456UR-IS-VGA-WIN10:1688 ESTABLISHED
TCP 127.0.0.1:52349         ASUS-A456UR-IS-VGA-WIN10:10402 TIME_WAIT
TCP 127.0.0.1:52351         ASUS-A456UR-IS-VGA-WIN10:10402 TIME_WAIT
TCP 127.0.0.1:52354         ASUS-A456UR-IS-VGA-WIN10:10402 ESTABLISHED
TCP 192.168.1.101:139      ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 192.168.1.101:40735    ASUS-A456UR-IS-VGA-WIN10:0 LISTENING
TCP 192.168.1.101:49684    hk2sch130020761:https ESTABLISHED
TCP 192.168.1.101:49800     111.221.77.142:40027 ESTABLISHED
TCP 192.168.1.101:49802     91.190.218.55:12350 ESTABLISHED
TCP 192.168.1.101:50514     203.104.174.13:https ESTABLISHED
TCP 192.168.1.101:52003     sc-in-f188:5228 ESTABLISHED
TCP 192.168.1.101:52233     server-54-230-150-220:https TIME_WAIT
TCP 192.168.1.101:52258     sa-in-f100:http TIME_WAIT
TCP 192.168.1.101:52260     sin10s07-in-f09:https TIME_WAIT
TCP 192.168.1.101:52264     104.31.72.126:http TIME_WAIT
TCP 192.168.1.101:52265     104.31.72.126:http TIME_WAIT

```

Analisis: Untuk yang streaming bisa di lihat bahwa paket data lebih banyak dari pada paket data pada kompas.com tadi. Dan pada CMD nya juga lebih banyak dari pada kompas.com. hal ini mungkin di sebabkan karena pada saat streaming membutuh kan bandwidth yang besar.